

驭数有道 用户至上

百度2020年数据安全、隐私保护与内容治理专项报告

驭数有道　用户至上

目录



前言

数字化浪潮席卷全球，数字经济已成为推动全球发展和社会持续转型的重要力量。信息化在带来智能便捷的同时，也引发了社会各界对数据安全和隐私保护的担忧。如何做到合理合法、有序有效地利用大数据，同时保护好个人隐私，已成为互联网行业行稳致远的关键命题。

百度始终坚持用户利益为先，严格遵守隐私保护和数据安全相关法律法规，建立三位一体的全面保障机制——通过制度化的数据保护策略、规范化的数据处理流程和智能化的数据安全技术，加强内容治理、保护网络安全，力求用户能真正感受到“信息被保护、意愿被尊重、服务有价值”，更放心地享受百度带来的便利和美好。

实现数据隐私保护需要强大的安全技术能力作为支撑。百度通过人工智能等技术，强化个人信息保护的技术内核，通过事前防范、事中保护和事后追溯，全方位保障用户数据安全。创新“隐私计算”技术，打破数据孤岛，让数据在保护隐私的前提下进行深度学习运算，实现“数据可用不可见”，释放数据最大价值。推进 AI 安全产品化，赋能生态伙伴，帮助伙伴提升数据安全防护水平及合规性。

数据数量急剧扩增和广泛连接，应用场景日益丰富，也对百度的内容治理提出了更高要求。百度持续完善综合治理体系，通过技术开源、协作互赢等方式，实现内容生产、分发及评价的全生命周期监督管控，为用户提供安全、高质量、可依赖的产品及服务，营造清朗健康、和谐高效的网络环境。

AI 技术在不断提升数据安全的同时，也带来了社会治理、伦理道德和隐私保护层面的全新挑战。百度坚持：AI 的最高原则是安全可控，AI 的存在价值是教人学习、让人成长。百度会防止 AI 滥用，让技术创新更好地造福人类，为人类带来更多自由与可能。

> “数字经济时代，个人信息保护关乎每个人的切身利益，更关乎社会公共利益。百度高度重视个人信息保护，将用户权益保护作为企业发展的核心竞争力，严格遵循数据隐私保护的价值观：同意（Consent）、透明（Clarity）、可控（Control）。
>
> 技术是百度的信仰。用技术改变世界，也用技术解决改变世界过程中遇到的各种困难和问题。在 AI 时代，百度正在持续开发各种针对隐私风险检测及防护的技术创新产品及工具，努力用科技的方式让隐私更安全。”
>
> ——百度集团资深副总裁 梁志祥

数字时代，每个百度人都将更深刻地认识隐私保护和数据安全对用户的重要性，以开放的姿态迎接创新，以共赢的态度进行交流，守护每一份来自用户的信任，为数据安全保驾护航！

本报告由百度 ESG 工作组编制，经百度 ESG 委员会批准发布，旨在向各利益相关方披露 2020 年 1 月 1 日至 2020 年 12 月 31 日期间百度在数据安全、隐私保护、内容治理方面的表现，以及百度针对 AI 时代的挑战和机遇所进行的思考和应对。这是百度发布的首份数据安全、隐私保护和内容治理的专项报告，也是 2020 年百度 ESG 系列专项报告之一。未来，我们会依照实际情况，再次发布该主题的专项报告。

大事记

2010 年 12 月
百度发起“打击互联网不良信息，共建和谐网络环境”的“阳光行动”。

2012 年 3 月
百度发布《数据安全策略》，数据安全被首次纳入百度安全管理体系建设。

2013 年 5 月
百度发布《网民权益保障计划》，成为全球首家宣布为网民提供先行保障的搜索引擎公司。

2015 年 11 月
百度成立安全委员会，强化百度数据安全顶层设计，落实安全职责。

2016 年 9 月
百度安全发布了业内首部《百度安全打击黑产白皮书》。

2018 年 5 月
百度董事长兼首席执行官李彦宏首次提出 AI 伦理四原则。
百度正式成立数据隐私保护委员会，承担数据合规管理责任，负责数据隐私相关重要问题的战略决策。

2019 年 10 月
百度自动驾驶信息安全防护平台获得 EAL4 级安全产品认证，这是目前自动驾驶软件安全防护领域最高等级的安全认证。

2020 年 6 月
百度联邦计算平台和 MesaTEE 通用安全计算平台两款大数据安全产品均被中国信通院授予“第十批大数据产品能力评测证书”。

2020 年 7 月
百度作为首批重点互联网企业和基础电信企业，签署了《电信和互联网行业网络数据安全自律公约》，向用户、行业与社会作出庄重的安全承诺。
百度智能云再次升级个人信息数据保护能力，完成 ISO/IEC 27701：2019 新版安全标准认证升级，同期获得公有云个人鉴权信息保护国际认证 (简称 “ISO 27018”)，成为国内首家通过该认证的云服务提供商。

2020 年 9 月
百度地图获得中国网络安全审查技术与认证中心颁发的首批移动互联网应用程序（App）安全认证证书。

2020 年 11 月
百度获得首批数据管理能力成熟度（DCMM- 国标）第四级 -“量化管理级”证书，代表了国内数据管理能力的标杆水平。
百度入选由中国信通院发起的“2020 年第二期网络数据安全合规性评估优秀案例”，形成最佳实践并在行业内推广。

2020 年 12 月
百度史宾格隐私合规检测安全平台获得“2020 年网络安全国家标准优秀实践案例”二等奖，是国内唯一入围该奖项的隐私合规检测平台。



用户权利

用户的合法权利在百度得到充分尊重和保护。

用户信息被保护、意愿被尊重

仅在获得用户同意后，百度才会以合理透明的方式使用其个人信息，同时给予用户充分的控制权。让用户切实感受到信息被保护、意愿被尊重。用户可登录百度隐私保护平台 http://privacy.baidu.com 或通过相关产品服务页面阅读隐私政策，全方位了解百度隐私保护的价值观与原则。

知情权

- 用户享有充分的知情权，可以清晰地获悉百度收集个人信息的目的。
- 用户可通过分栏式的页面设计阅读百度隐私政策，并能够在加粗字体提示下阅读重要条款，以更好地了解百度如何收集、使用数据。

选择权

- 用户有权利选择是否提供个人信息。只有在用户授权后，百度平台才会进行信息收集，绝不会进行强制收集。当个人信息处理目的发生变更时，百度会在处理前通过合理方式提示用户再次进行授权。

控制权

- 用户对个人信息拥有修改、删除的权利。用户可随时通过开 / 关权限的方式实现授予或撤回同意的权利，权限控制设计一般在产品页面中，易于操作。应用户有效请求或信息保存期限届满，百度将依法删除用户个人信息或停止处理个人信息。
- 用户在产品使用过程中，如果希望编辑个人基本资料、更改密码、添加安全信息或设置关联帐号，可以通过一站式帐号管理平台 https://passport.baidu.com/ 进行相应操作。如果有其他个人信息保护相关问题，也可通过统一的反馈专用渠道 http://help.baidu.com/personalinformation 或各产品页面展示的入口与百度取得联系。

便捷通路及时响应用户诉求

用户在使用百度平台过程中遇到任何问题均可随时反馈，最快可在 20 秒内得到极速响应。在不断优化用户体验的同时，百度也会根据用户的核心需求不断升级和完善相关产品。

数据：2020 年

百度用户反馈入口已接入 **200** 条产品线

并覆盖 **1,231** 个产品端

累计处理用户反馈超过 **8,000** 万起

用户反馈信息处理率高达 **100%**

用户对反馈处理的满意率高达 **92%**

多元反馈渠道

- 用户在使用百度 App 时，若遇到资讯内容出现“标题党”、质量低下、错别字或虚假广告等情况，可以点击新闻或广告右下角的“×”进行“举报反馈”，或通过个人中心的“帮助与反馈”页面进行反馈并跟进处理状态。用户也可以直接通过百度用户服务中心 http://help.baidu.com 进行一站式举报或通过 400-921-3900 热线联系百度人工客服，获得即时反馈和帮助。





图：用户进入“举报反馈”页面，对问题内容进行反馈



图：用户可点击“咨询问题”进行提问，或点击“反馈建议”留言

持续优化反馈体验

- 通过百度内部一站式反馈处理标准流程，用户的大多数问题都可以实现多视角的深入分析、多人同步更新处理状态，确保及时响应用户关切。
- 2020 年，百度进一步优化用户体验，反馈方式从传统的留言形式过渡到在线人工客服响应形式。该功能上线后率先在百度网盘投入试点运行，部分用户可通过与人工客服的即时互动得到实时反馈。

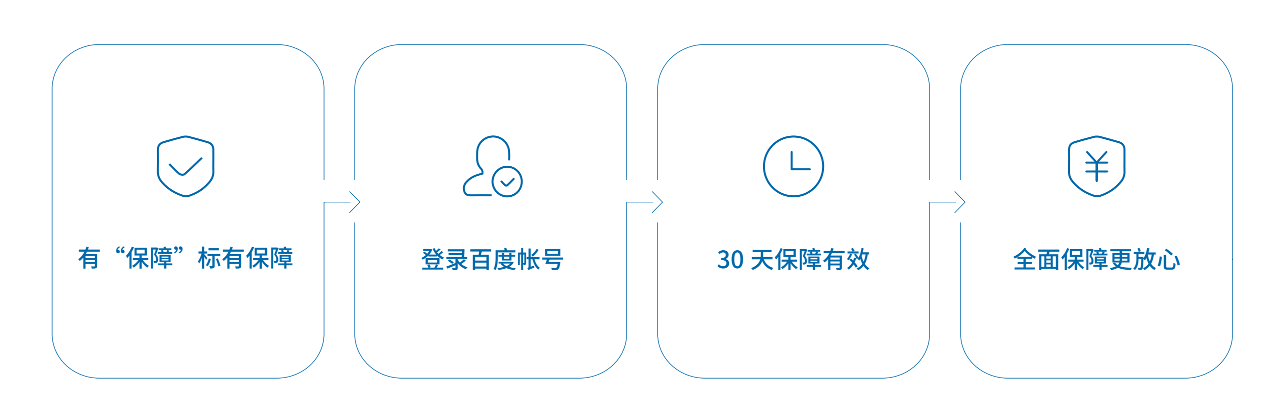
全额先行赔付让用户放心搜索

用户在搜索信息、进行网上购物时可参考“官方”和“保障”标识，以快速识别官方网站及百度保障范围内的网站，降低搜索风险。



图：部分搜索结果添加“保障”标识

- 用户登录百度帐号，点击带有“广告”或“保障”标识的搜索结果，如因假冒官网或钓鱼欺诈而蒙受经济损失，可通过“百度网民权益保障计划”申请赔偿。通常在提交反馈信息后 2 个工作日内，用户即可获得响应；5 个工作日内收到判定结果；在符合保障覆盖范围的情况下，20 个工作日内即可领取保障金。若百度客服无法判定纠纷结果，将引入第三方机构人民调解委员会，协同线上线下解决服务纠纷，使用户权益获得更完善的保障。
- 2020 年，该项举措再次升级完善，保障覆盖范围进一步扩大，且赔付金额在部分行业进一步提高。



图：百度网民权益保障计划

数据：2020 年

用户共通过“百度网民权益保障计划”提交申请 **20,000** 余起

百度协调商家为用户退款 **16,110** 余起

退款总额达到 **721** 万余元



案例

网民购买迪士尼门票受骗，获赔 3,380 元

鲁女士通过百度搜索到某售卖上海迪士尼门票的商家，并购买了 VIP 免排队服务套票。但鲁女士到迪士尼后发现根本没有免排队服务，套票也无法使用，且无法与商家取得联系。确认被骗后，鲁女士通过“百度网民权益保障计划”进行投诉，获得百度保障金 3,380 元。同时，百度曝光该存在欺诈行为的商家信息，并将其下线，避免其他消费者受骗。



平台责任

百度积极承担平台责任，遵守数据安全和个人信息保护相关的法律法规，积极落实相关举措，持续完善数据管理体系，建立三位一体的全面保障机制。通过制度化的数据保护策略、规范化的数据处理流程和智能化的数据安全技术，加强内容治理、保护网络安全。

个人信息保护遵循四大原则

百度在整个数据收集、存储、加工、使用、提供等过程中，将合法、正当和必要作为前提标准，要求隐私保护规划与业务规划同步进行，隐私影响评估和隐私防护措施与个人信息处理动作同步上线，确保在整个数据生命周期中持续落地隐私保护的基本原则。

知情同意

- 百度系 App 会依法依规发布对应的隐私政策或隐私条款，以易懂的语言，明确地向用户告知所收集个人信息的处理目的、方式、范围、安全保障措施、权利救济渠道等，确保用户是在充分了解百度各产品的数据处理规则后同意与授权。同时在特定的创新场景中，通过友好的页面设计让用户深入了解数据处理情况。如涉及个人数据的共享，百度依法依规保障用户知情权，并在用户授权范围内进行数据处理。





图：百度地图隐私政策

最少够用

- 百度确保信息使用不超过必要的限度。用户个人数据的收集、存储、加工、使用、提供等环节均在业务需求的必要范围内进行。

用户体验

- 百度通过清晰简明的信息管理工具和页面选项，向用户展示信息变更、权限授予、帐号关联及注销等控制功能，优化用户体验。

安全保障

- 公司内部管理流程形成从数据资产识别、数据分类分级、数据申请及授权、行为审计到报告的闭环。在实施过程中，百度严格遵守《百度数据安全策略》，以隐私合规设计（PBD，Privacy by Design）和隐私风险评估（PIA，Privacy Impact Assessment）为抓手，打造贯穿业务始终的评估机制。在技术工具上，在数据处理过程中，运用脱敏、加密及差分隐私保护等技术手段进行去标识化，保护隐私数据。此外，针对用户个人敏感信息的处理，百度实现了在系统、存储、服务等各个层面精确到个人的身份认证及访问控制。

多维立体全面保障策略

百度制定一系列内部管理制度，覆盖百度及其分公司的所有员工，通过顶层治理架构、安全风险管控体系和安全审计机制，全方位、全流程保障数据安全。

委员会机制确保流程高效、合规

- 百度完善网络安全治理组织架构，安全委员会、数据隐私保护委员会、数据资产管理委员会三大委员会各司其职、相互制约，以保障数据处理的透明度和安全性，更有效地控制数据安全和隐私风险。

数据安全：安全委员会

百度安全委员会作为公司顶层安全组织，统一负责产品、数据及个人信息安全范畴的风险控制决策、资源投入以及各团队协调工作，确保公司的信息安全、产品安全、数据安全，让用户及客户安全地获取所求。百度安全委员会主席是百度首席技术官王海峰。

隐私保护：数据隐私保护委员会

百度建立自上而下的隐私保护体系，顶层组织为数据隐私保护委员会：一方面负责数据隐私相关的重要战略制定、问题决策；另一方面承担着用户数据保护、跨境数据合规等管理责任，确保百度数据隐私的举措符合国际条约和国家相关政策法规的要求。

数据治理：数据资产管理委员会

在公司整体数据架构层面，百度设有数据资产管理委员会，成员由大数据部、安全部、法务部、搜索等业务线代表组成，负责数据资产相关政策、管理规范、机制和流程等的制定、发布和决策。

业务与职能分工合作、落实安全责任，管控安全风险

- 百度建立了安全委员会、安全工作组及各部门安全负责人三个层级的安全组织保障架构，以有效控制安全风险，提高管理效率。

基础防守

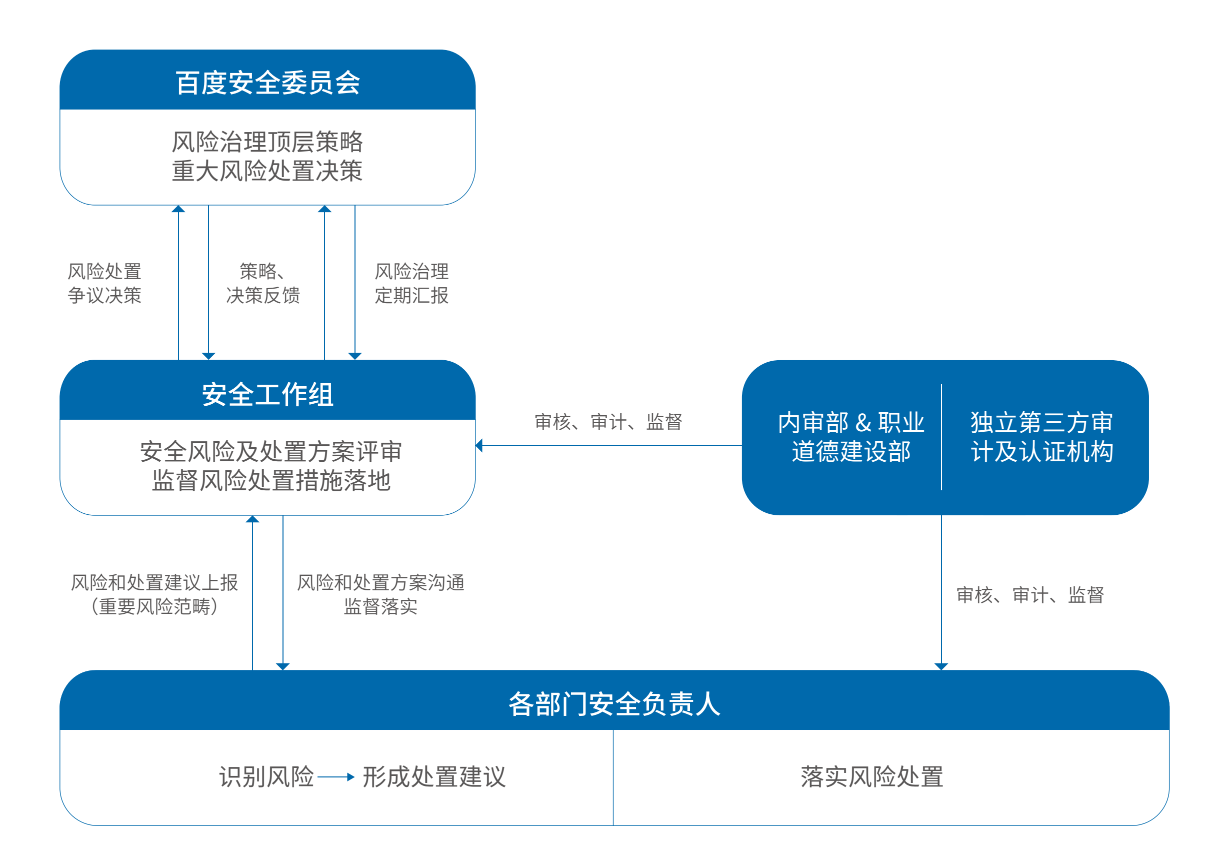
作为百度信息及产品安全的控制执行方及第一责任方，由部门主管担任部门安全负责人，贯彻执行公司的信息安全相关策略、措施。

攻防对抗与威慑

作为安全风险预防与监察方，由安全部等多部门共同组成安全工作组，负责公司层面各项安全工作的协调开展，并定期向百度安全委员会进行工作汇报。

稽查、内部审计

由百度内审部与职业道德建设部组成，基于公司信息安全管理现状，针对重大信息安全风险开展审计、检查，并负责接收、调查和处理安全问题中涉及违反职业道德、违反公司信息安全相关制度与流程的情况。



图：安全组织保障架构

完善审计机制，推进安全审计全覆盖

- 百度定期开展安全相关的常规审计和第三方认证审计与评估，实现对公司数据安全和隐私保护措施的客观评估与全面监督。

常规内部审计

由百度内审部针对公司数据安全和隐私开展专项审计工作，做出风险提示并提出缺陷及问题，并针对异常情况进行追溯审计。

第三方认证审计

百度核心系统均已完成第三方国家信息系统安全等级保护三级评测，部分重要核心系统通过了四级评测。此外，百度云、百度网盘等百度的主要业务或产品均开展了 ISO/IEC 信息安全相关的专业资质认证审计检查工作。

第三方安全评估

每年由专业的第三方安全机构在遵循道德规范的前提下进行双盲测试（double blind test）[1]或单盲测试（blind test）[2]，用以测试安全防御和响应体系的薄弱点及运行有效性。

助力安全文化人人参与

- 百度持续加强员工安全教育，制定了覆盖全员（包括公司管理层、正式员工、实习生与劳务派遣等非正式员工）的立体化培训机制，以提升员工安全意识、素养和技能。

培训活动

开展直播、在线课程、线下专业课等各种形式的安全专题培训活动。专设安全宣传月，对安全知识进行场景化宣贯。

意识考核

每年至少开展一次全员强制性安全及隐私意识考核（满分通过制）。

攻防演练

在全员范围内定期进行安全意识的攻防演练，通过模拟外部攻击来检验员工对常见攻击的抵御能力，针对性地提升员工的安全意识。

数据：2020 年

线上安全培训总体学习规模
超过**50,000**人次

学习课程超过
100 门

新员工安全意识培训
32 次

开展攻防演练
2 次

全意识巩固专题强化培训考核
5,242 人次

1 双盲测试：指对评估方不提供任何评估测试信息，对被评估方不事前通知时间、地点和评估内容的前提下进行的评估检测方法。
2 单盲测试：指对被评估方不事前通知时间、地点和评估内容的前提下进行的评估检测方法。

强化以 AI 为核心的安全体系

百度强化技术手段，提升个人信息保护及防护能力。通过人工智能等技术，建设全生命周期网络内容管理机制。

围绕 Security、Safety 和 Privacy 三大维度建立安全 AI 生态

- 百度深化自主研发，以技术赋能网络安全建设，从 Security、Safety 和 Privacy 三个维度对安全问题进行考量，研发部署了一套覆盖云、管、端的多层次数据管理及安全保护方案。

Security：解决由于物理世界和数字世界的攻击所造成的 AI 系统在工作过程中出现误判的问题

安全技术范例	
安全技术范例	内核漏洞热修复技术 OASES KARMA：避免"生态碎片化"导致安全漏洞被不法分子利用
	MesaLock Linux 内存安全操作系统：提升 Linux 生态安全性
	大规模图数据库 HugeGraph：秒级关联查询能力，用于欺诈检测、关联分析、知识图谱和数据治理等场景
	嵌入云应用执行引擎 Open RASP：监控和保护数据库
	深度伪造检测 DF Detection：提高 AI 检测识别准确率，从源头阻断滥用 AI 换脸技术实施电信网络诈骗等违法行为
	安全 OTA：为智能设备提供云、管、端全链条解决方案，系统更新、功能迭代和漏洞修复都能第一时间触达设备

Safety	避免光照、空间变幻、模糊、噪声和天气多变等真实世界环境因素变化对模型分类和预测造成负面影响
安全技术范例	模型鲁棒性体系化评估框架： 根据变化的任务场景制订评估标准，量化潜在的安全威胁并确认系统在非预期工作场景中是否误判
	AdvBox 对抗样本工具箱： 优化主流机器学习平台，以快速提升模型的健壮性

Privacy	覆盖数据采集、处理、流通、计算全生命周期的个人信息安全防护
安全技术范例	安全通信库 MesaLink TLS： 规避内存安全漏洞导致的用户隐私泄露
	下一代可信安全计算服务框架 MesaTEE： 为云上数据的完整性和保密性提供芯片级安全保障
	安全联邦计算平台： 基于多种安全技术的联合计算平台为亿万级数据联合分析、联合风控、联合营销提供安全保障
	差分隐私： 数据采集或发布前，对数据进行扰动添加噪声，隐藏真实数据，避免攻击者通过猜测获取数据
	AI 自动脱敏： 集成百度先进的图像识别、自然语言处理等 AI 能力，通过敏感数据智能扫描发现，快速了解敏感数据资产分布；通过自定义脱敏策略实现多元敏感数据的脱敏处理，助力解决复杂业务场景的敏感数据保护



案例

打造云上智能一体化安全体系，守护云端数据安全

在云安全领域，百度引入联邦计算、可信计算等一系列 AI 安全技术，将领先的 AI 安全能力与百度智能云深度结合，实现企业云上防御体系智能化、一体化的安全升级。

百度发布智云盾，集合本地快速检测、自动化拓展 T 级云防、黑客攻击检测、实时安全防御和威胁情报等一系列技术能力，为互联网数据中心（IDC）提供完备、便捷的安全基础设施。并于 2020 年下半年发布“智能数据安全网关”和“智能威胁狩猎平台”，提供云端一站式敏感信息探测、脱敏、审计等安全管理系统，有效应对攻防对抗等场景，进一步保障云端系统数据安全。

系统化守护 网络安全运营

- 百度以 AI 为核心，大数据为基础，不断提高网络安全感知、防护与应急处理能力，创造安全稳定的网络环境。

产品安全质量

百度是 DevSecOps[3] 安全理念的践行者，围绕百度产品研发的全生命周期及研发工具，提供具备全链条安全保障的解决方案。在产品需求设计、编码、测试、上线的各个环节，通过安全协同、安全前置、安全自动化等措施，提升研发效率，保障百度产品安全质量

安全预案演练

定期组织安全预案演练，确保核心工作人员在系统漏洞、网络攻击、网络侵入等安全事件发生后可有效处置

系统风险识别

主动进行攻防测试，识别当前系统的缺陷和风险

监控报警及阻断

对基础安全及纵深防御检测能力实施监控报警，及时阻断异常和攻击行为

异常行为追溯

对端到端的核心数据使用行为进行检测与审计，对于异常行为进行追溯

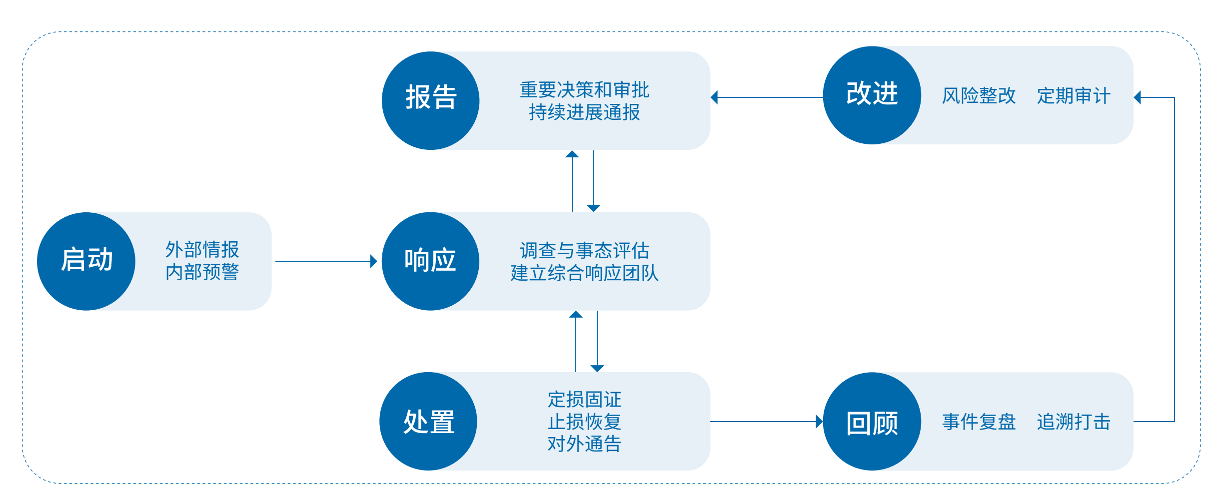
安全提示标注

对存在可能被劫持、恶意篡改、访问状态不稳定等异常情况的网站进行安全识别和风险提示，规避用户使用风险

图：网络安全综合防护方案

3 DevOps 标准即《研发运营一体化（DevOps）能力成熟度模型》，是由中国信息通信研究院牵头，联合国内外行业顶尖企事业单位专家共同制定，目前已在联合国直属标准化组织 ITU-T 正式立项。主要包括敏捷开发管理、持续交付、技术运营、应用架构、安全及风险管理、系统和工具等部分的评估。DevSecOps 将安全因素融入敏捷开发和 DevOps 过程中，力求无缝衔接，公开透明。

- 日常运营环节，百度构建并持续优化网络安全综合防护方案，提高对漏洞防护的适应能力。面对突发网络安全事件，百度建立了完善的安全事故应急处理机制，将事故负面影响最小化。
- 针对影响数据安全，已经或可能对个人信息产生影响的安全事件，百度建立了启动、响应、上报、缓解、解决、追溯取证和通知等一整套规范的安全事件管理流程及应急预案。
- 根据安全事件的具体性质不同，响应角色由多个专业部门及专家团队组成和参与，坚持以“在最短的时间内消除或降低风险对组织、业务及用户 / 客户产生的负面影响”为根本原则。根据事件的影响、范围及可控性，百度将安全事件程度从高到低划分为一级、二级、三级。



图：百度安全事件响应流程

- 百度同时设立了百度安全网站 http://anquan.baidu.com，百度安全社区 http://anquan.baidu.com/forum，百度安全应急响应中心 http://bsrc.baidu.com，以帮助用户获取安全信息，促进安全专家的合作与交流。



案例

安全应急响应中心，联结产业和白帽子的纽带

百度安全应急响应中心 https://bsrc.baidu.com/v2/#/home 是百度安全漏洞收集及应急响应平台。该平台致力于维护互联网健康生态环境、保障产品和业务线的信息安全、促进安全专家的合作与交流。

近年来，安全应急响应中心先后举办“百度大学生网络安全技能大赛”“安全应急响应中心年度盛典”“白帽之夜”“高校网络安全技术分享”等交流活动，并联合国内 41 家最主要的应急响应中心发起了 DEF CON CHINA 志愿者计划，为中国下一代网络安全人才的培养搭建平台、贡献力量。同时，作为持续性活动的一部分，安全应急响应中心也推出了多项漏洞悬赏奖励计划，并针对 AI 时代的新场景、新风险开展了智能设备安全众测挑战，高质量漏洞的最高奖金达到 100 万元。

“AI+ 人工”综合治理违法信息

- 百度持续加强产品内容和商业推广内容治理，建设全生命周期网络内容管理机制，确保高效处置违法违规信息，营造健康向善的网络环境。

事前监控，事中拦截，事后追溯流程

百度构建“AI 机器审核 + 人工复检 + 人工巡检”的风险防控体系，综合利用多种算法和训练模型，打造防御闭环，提升用户的搜索体验。

阶段	内容风控	商业推广
事前监控	• 搭建基于搜索生态的安全感知系统，广泛收集信息，进行智能建模和“7X24”小时监控，筛选黄、赌、毒、虚假夸大、隐私侵犯等违法违规信息，对违法违规内容进行驳回或下线处理	• 建立事前审核机制，严格审核广告商准入资质，不断强化广告内容审核能力（机器 + 人工）严禁风险广告投放 • 对高风险行业实施落地页托管，加大托管页面审核力度，避免落地页被篡改
事中拦截	• 综合利用技术识别和人工巡查对内容进行审核管控，甄别恶意内容和不良信息，并通过拒绝、风险标注、拦截提示、搜索屏蔽等措施进行处置	• 对已上线广告和落地页进行技术巡查，对违规内容进行下线处罚，以多重审核方式对内容进行审核过滤
事后追溯	• 利用百度深度学习模型和知识图谱对规模化、系统化、跨境化的违法违规内容进行追踪溯源 • 对违规帐号采取警示、拒绝发布、删除信息、限制功能、暂停更新等处罚措施	• 进行合规验证，杜绝广告内容篡改，若发现有害广告，进行下架处理，并对其广告账号进行关停

数据：2020 年

百度共计屏蔽处置色情、赌博以及危害社会安全等违法违规信息共计 **516.2** 亿余条，其中机器屏蔽处置 **515.4** 亿余条，人工巡查删除处置 **8,000** 万余条。

封禁违规用户共 **713** 万

累计拒绝各类违法违规广告超过 **22.98** 亿条

事后处罚阶段百度共处罚违规广告帐号 **28,031** 个

累计拦截屏蔽“涉嫌窃取公民个人信息”恶意网站 **2.47** 万个，网址 **11.2** 万个

总计拦截恶意网页触达总量 **939** 万个

针对“身份证、银行卡”两卡交易信息累计清理 **493** 万次



案例

重点监管医疗信息，助力营造良好就医环境

百度对医疗信息重点监管，加强技术巡查，为用户构建优质的就医信息查询渠道。医疗信息只有经严格审核后才可正常推广，确保权威就医信息置于搜索结果首位，为建设网络诚信医疗体系贡献百度力量。2020 年，共计 14.6 万余家公立医院的官方网页在百度搜索渠道优先显示；百度针对病症词、药品词、医疗机构类等 55 万个敏感词汇加注风险提示信息。

AI 核心技术为个人隐私护航

- 在隐私保护与数据安全层面，百度将一系列访问控制及隐私增强技术应用于数据收集、存储、加工、使用、提供的全生命周期，保护用户隐私的同时释放数据价值。
- 百度以先进的人工智能技术为支撑，深度贴合国家监管标准，打造“史宾格安全及隐私合规平台”，将隐私基准测试纳入上线前检测流程。作为业界首款对外提供服务的 App 收集使用个人信息合规风险检测和治理系统，“史宾格安全及隐私合规平台”旨在帮助 App 开发和运营企业快速对标国家、行业安全标准与规范，精准识别和检测包括隐私政策文本、App 收集使用个人信息行为、App 用户权利保障等方面的隐私合规风险，实现检测能力与监管要求的一致性，助力自查整改，保障用户隐私安全。目前，百度旗下主要 App 和 SDK 均已完成对该平台的接入和内部检测。

AI 的挑战和机遇

面对 AI 时代的风险和挑战，深化理解 AI 伦理、建设全行业共赢共生的安全生态是解决 AI 与人类共存问题的必由之路，也是百度前行的指引和方向。



“三维一体”的 AI 化公司

近年来，随着 AI 核心技术取得诸多突破，AI 时代对社会治理、伦理道德、隐私保护等方面的挑战也随之而来，仍需持续开展研究和预判。

法规层面	当前法律存在一定程度的不适用性，有待形成完整的 AI 法律法规体系
标准层面	AI 数据安全通用标准和细分应用领域亟待完善
企业层面	逐步改进合规要求的顶层设计及实施细则，将伦理意识和文化落实到企业风险管理体系中
技术层面	应对技术发展相对不成熟，风险评估能力仍有提升空间

图：人工智能技术的伦理风险[4]

- 作为 AI 技术的开发者和应用者，百度一方面致力于 AI 创新技术的开发，一方面也密切关注 AI 新技术可能带来的负面影响和社会问题。发展可信、可控并使人类最终受益的 AI 技术，是百度的责任担当和使命感的表现。

- 百度董事长兼首席执行官李彦宏提出了 AI 伦理四大原则，即 AI 的最高原则是安全可控；AI 的创新愿景是促进人类更平等地获取技术和能力；AI 的存在价值是教人学习，让人成长，而非超越人、代替人；AI 的终极理想是为人类带来更多自由与可能。百度 AI 伦理四大原则旨在针对所有人工智能新的产品、技术建立一个全社会共同遵循的理念和规律，解决人工智能与人类共存的矛盾问题。只有坚持安全可控的最高原则、建立完善的人工智能伦理规范、加快人工智能伦理原则落地，才能让人工智能技术实现多元共治、普惠更多群体，实现社会的可持续发展。

4 参考国家人工智能标准化总体组《人工智能伦理风险分析报告》

- 针对 AI 技术带来的新兴风险，百度持续加强内部合规治理、提倡社会伦理道德价值观，并针对性地开发反欺诈、深伪鉴别等技术方案，以最大限度地趋利避害。此外，为了防止 AI 技术被滥用，针对具体的 AI 技术应用场景、对外合作及 AI 技术输出，百度会进行相关风险的事先识别评估及风险防御设置，通过采取相适应的风险防控措施，以有效控制风险实际产生的损害后果。

- 在 AI 伦理原则和标准体系的建构方面，持续跟进标准化相关的提案，参与编写了国家人工智能标准化总体组的《人工智能伦理风险导论》; 与信通院联合编制《人脸识别技术在 App 应用中的隐私安全研究报告》; 参与《车联网信息服务用户个人信息保护要求》行业标准编写与发布。国际交流方面，参与 AI4SDGs[5] 公益研究计划和国际协作网络，并资助其公益研究课题，积极推动人工智能的人才培养和技术善用，凝聚全球共识。



案例

构建 Apollo 无人车安全驾驶体系，保障信息安全

信息安全的挑战是伦理领域的难题，也是无人驾驶技术必须跨越的门槛。百度聚焦于自动驾驶核心技术，高度重视其潜在安全风险挑战，将 Apollo 信息安全核心目标定位为“防御外部入侵，防范核心应用、防护隐私数据泄露，防止控车威胁”。

百度成立 Apollo 汽车信息安全实验室，专注于汽车信息安全技术的分析以及趋势跟踪，涵盖数据隐私保护、自动驾驶信号伪造对抗等十多个智能驾驶信息安全方向，应用 AI 技术，构建智能网联汽车“检测—保护—响应—恢复”全生命周期的信息安全体系；同时，百度着眼于技术防护、数据管理、政策标准三方面，兼顾用户驾驶数据、交通参与者个人信息保护和防止自动驾驶汽车被黑客攻击和控制的能力。

打造智能设备生态安全体系，保护用户隐私数据

在万物互联的智能语音时代，小度助手已提供超过 62 亿次的语音交互，如何保护用户数据成为信息安全关注的重点。

百度以“风险可控、安全可靠”为目标，构建覆盖云、管、端的多重纵深防御体系。应用 AI 技术，依托可信执行环境、安全 OTA（空中下载技术）、系统热修复等安全方案，同时兼顾设备安全及数据安全，建立“及时感知、快速阻断、安全更新”的保障闭环，形成事前、事中、事后的全过程控制。

此外，百度积极参与智能设备行业标准建设，基于智慧酒店场景及互联互通场景，对外输出最佳安全实践，全面保障智能设备生态安全、保护用户隐私安全。

5 AI4SDGs：面向可持续发展的人工智能

构建开放包容的 AI 生态

AI 时代面临的安全挑战比传统时代更复杂，维护 AI 时代的网络安全是全社会的共同责任。百度崇尚“Everyone Can AI”的理念，积极鼓励公司对外开源 AI 相关技术工具，以更开放的态度，与广大网民、行业协会、科研机构、社会组织等利益相关方沟通协作，在开放包容、多元互鉴中寻求共赢，共筑网络安全防线，共同打造 AI 时代的安全生态，持续为人工智能领域蓬勃发展贡献力量。

参与产业联盟与行业标准制定

- 百度积极加入标准组织与产业联盟，以深厚的技术沉淀与多方开展技术合作，贡献中国智慧，与产业伙伴一同推进安全生态建设。

- 百度先后加入了 ISO/IEC JTC1[6]、ITU-T[7]、IEEE-SA[8]、TC28[9]、TC260[10]、CCSA[11]、CCSA-TC601[12]等国内外重要标准化组织。在 TC260 组织下，参与制定《信息安全技术 移动互联网应用程序（App）个人信息安全测评规范》《信息安全技术 移动互联网应用（App）收集个人信息基本规范》《信息安全技术 互联网信息服务安全通用要求》《信息安全技术 网络数据处理安全规范》等 30 余项国家标准，议题覆盖 AI 安全、黑产打击、App 隐私合规、数据安全及隐私保护等众多网络安全领域。

- 作为 CCSA-TC601 成员，百度积极参与《数据资产管理实践白皮书》《大数据服务能力成熟度模型》《数据治理标准白皮书》等多项大数据领域白皮书或标准制定。2017 年 11 月，百度联合华为、中国信息通信研究院发起“智能终端安全生态联盟（OASES）”，与产业伙伴共同推进安全生态建设。

- 国际标准方面，百度深度参与编写全球首个 DevOps 标准，即《研发运营一体化（DevOps）能力成熟度模型》，并获成员单位正式授牌。

推进产学研合作

- 百度积极助力产学研一体化，探索产学研互促新模式，与复旦大学等多所外部高校开展合作，就数据和隐私保护相关热点展开研究，并在“移动应用生物信息泄露分析”“百度及周边产品安全漏洞分析”等领域取得突破性进展。

- 百度以飞桨深度学习平台为代表的人工智能开源平台作为创新基座助力人才培养，目前已构建起涵盖学习、实践、比赛、认证、就业在内的全周期服务体系，使人才在实践中得以培养，使前沿技术落地课堂。截至 2020 年 12 月，百度已经培养 AI 人才超过 100 万，未来 5 年百度还将培养 500 万 AI 人才，为中国智能经济和智能社会的发展提供 AI 人才保障。

案例

开源飞桨赋能社区

百度飞桨以百度多年的深度学习技术研究和业务应用为基础，是中国首个自主研发、功能完备、开源开放的产业级深度学习平台。其集深度学习核心训练和推理框架、基础模型库、端到端开发套件和丰富的工具组件于一体，能够不断降低学习门槛，让开发者和企业安全、快速地实现自己的人工智能想法，为人工智能产业大规模化提供了坚实的基础。

2020 年 12 月 20 日，在 WAVE SUMMIT+2020 深度学习开发者峰会上，飞桨全新发布 PaddleHelix 螺旋桨生物计算平台；推出业内首个通用异构参数服务器架构。其开源算法库全面升级，官方算法数量从 140+ 扩展至 200+；硬件生态伙伴达到 20 家，适配或者正在适配的芯片 /IP 型号共 30 种，与国产芯片的适配数量保持领先地位，持续打造软硬一体、自主可控的 AI 技术底座，加速人工智能产业生态构建的步伐。

如今，飞桨开发者生态已经凝聚了 265 万开发者，在开源社区中有超过 5,000 位开发者为飞桨做出贡献。经过层层筛选后，有 97 位优秀的开发者成为了飞桨开发者技术专家（PPDE）。飞桨还成立了 7 个特别兴趣小组，在全国范围内，已经有 132 个城市和高校自组织社区在主动自发举办飞桨社区活动。

在产业应用方面飞桨服务了 10 万企业，基于飞桨平台创造了 34 万个模型，覆盖到了金融、教育培训、交通出行等各行各业。

在人才培养方面，飞桨师资培训覆盖到 500 所高校，支持了 200 多所高校开设学分课程，飞桨的 AI 大赛遍及全球五大洲 22 个国家，580 所高校。由于疫情原因，2020 年飞桨加大了线上直播课程的投入，共计开设了 176 次直播课程，在 AI Studio 学习与实训社区上进行学习的人次超过 290 万。

开展用户及供应商培训

- 百度为切实维护用户合法权益、鼓励用户依法维权，不定期开展线上及线下网络安全教育，传递网络安全知识，使用户规避网络安全风险。同时百度高度关注供应商网络安全认知水平与风险管理能力，要求其具有高效甄别数据是否合法提供的能力。

6 国际标准化组织 / 国际电工委员会第一联合技术委员会
7 国际电信联盟电信标准化部门
8 电子和电气工程师协会标准委员会
9 全国信息技术标准化技术委员会
10 全国信息安全标准化技术委员会
11 中国通信标准化协会
12 中国通信标准化协会大数据技术标准推进委员会



未来展望

保护数据安全与用户隐私、加强内容治理，百度责无旁贷

保护数据安全和个人隐私是一场持久战。数字时代，面对层出不穷且日益复杂的网络安全问题，如何利用技术手段拓展 AI 时代数据协作的信用边界，如何规避公民个人信息在流通过程中的泄露风险，是百度与监管机构、司法部门、科研学术机构将要共同面对的严峻挑战。

展望 2021，为保障网络安全健康发展，百度以高度的自觉和勤勉严谨的态度恪守相关法律，密切关注数据安全与隐私保护合规领域的立法动态，及时调整相应的产品策略、技术设置及信息处理流通环节，以更好地平衡数字时代下个人信息保护与大数据合理使用之间的关系，做用户权益的捍卫者。

百度将继续通过人工智能创新技术的研发与开源，不断加强新一代技术在全网数据安全与内容综合治理中的应用，提高安全防护能力以及内容识别的有效性、准确性；将继续以开放共赢的心态加强与政府、行业、学术机构的多层次协作，形成网络安全生态多方治理格局，在为用户创造价值的同时，营造清朗的网络空间环境。

面对 AI 的持续发展为法律、伦理、社会带来的重大挑战，百度将进一步致力于让更安全的 AI 驱动产业互联网的变革，以技术赋能、标准驱动、生态共建为支点，努力构建 AI 安全开放生态；积极应对算法偏见、隐私侵犯、数据保护、网络安全等一系列问题，持续加强 AI 伦理和治理研究，加强国际合作，贡献百度智慧和百度经验。

科技为更好，这是科技存在的意义，更是每一个百度人不分昼夜而努力追寻的目标。百度愿携手用户，通过为数据赋能新价值，一起重新认识和创造这个崭新的时代。

附录

百度数据安全和隐私保护制度

百度在数据安全、隐私保护、内容治理等层面制定了多项规章制度。所有规章制度在全公司范围内强制执行，并覆盖所有分公司。

安全红线及产品安全相关制度

百度严格遵守《中华人民共和国网络安全法》等适用的国家相关法律法规，内部设有《百度安全红线》《百度信息及产品安全处罚细则》《百度办公网络使用安全策略》《第三方合作项目安全规范》《百度安全问题处理总则》等多项规章制度，覆盖安全红线、办公安全、基础安全、数据安全与隐私、产品安全、第三方合作安全、安全管理等维度。

数据资产管理相关制度规范

为保护数据资产及用户个人信息安全，明确公司对于数据全生命周期的安全管理策略及原则，百度制定覆盖整个产品服务生命周期的数据资产管理规范框架体系，涵盖数据治理策略，数据权限、元数据、数据流通、数据价值评估、数据安全、数据合规等多项制度规范，包括《百度数据权限管理规范》《百度元数据规范》《百度数据质量治理最佳实践指南》等。

隐私保护相关制度规范

为实现隐私保护在产品中的落地和应用，百度制定《百度隐私政策总则》《百度用户个人信息保护合规总则》《百度用户信息展示安全规范》等规范标准，并为百度地图、百度网盘、百度贴吧、百度输入法等产品或服务制定公开单独的隐私政策。

网络内容治理相关政策标准

百度持续完善网络内容治理相关标准，为严厉打击有害信息提供内容依据，并为确保内容的准确性、公正性、真实性、合法性，制定严苛的审核标准。

商业风控	产品内容风控
《百度广告禁推管理政策》	《百度内容生态管理规范》
《商业广告提交手册》	《百度内容生态治理有害信息通用审核标准》
《广告内容审核管理制度》	《百度内容信息安全管理制度》
《信息发布审核制度》	《优质内容推荐机制》
	《信息发布审核制度》
	《百度信息内容实时巡查制度》
	《百度网络谣言打击和辟谣制度》
	《百度黑产产业链信息处置制度》

权威安全认证

百度为实现网络服务合规性，相继通过一系列国际及国家安全认证和评级。

认证类别	取得认证
数据安全及隐私保护认证	ISO 27018 公有云个人信息保护管理体系 ISO 29151 个人数据隐私保护管理体系 云服务用户数据保护能力（公有云） 云服务用户数据保护能力（私有云） PCI-DSS 支付卡行业数据安全标准（金融云） ISO 27701 隐私信息管理体系 BS 10012 个人信息安全安管理体系
信息安全认证	ISO 27001 信息安全管理体系 网络安全等级保护四级 网络安全等级保护三级 网络安全等级保护二级 ISO 22301 业务连续性管理体系 ISO 27017 云安全管理体系 CSA STAR 云安全国际认证体系 ISO 27032 网络空间安全管理体系 MTCS 新加坡多层云安全
产品质量体系认证	ISO 9001 质量管理体系 ISO 20000 信息技术服务管理体系
其他认证	SOC TYPE 1/2 报告系统与组织内部控制报告 CMMI 证书（能力成熟度模型集成 1.3 版本的 3 级评估） DCMM4 数据管理能力成熟度（DCMM- 国标）第四级 - “量化管理级” ITSS 云计算服务能力评估二级（公有云） ITSS 云计算服务能力评估二级（私有云） 云计算风险管理能力评估 EAL4 级安全产品认证

用户常见问题

综合梳理用户反馈的相关问题后，百度将用户在隐私保护和数据安全方面关心的问题整理如下：

百度会收集哪些用户信息？收集用户个人信息目的是什么？

百度会根据隐私政策披露的情况收集、使用用户信息，各产品 / 服务收集、使用用户个人信息目的可能因业务功能不同有所差异，建议使用前通过 https://privacy.baidu.com/ 查阅具体产品 / 服务的隐私政策内容。

如何注销百度帐号？注销帐号后用户信息去哪里了？

在百度 App 登录帐号，点击“设置”—“帐号管理”—“帐号注销”，系统会根据帐号情况显示能否注销。如满足注销条件按照提示点击下一步，验证帐号绑定手机或人工刷脸验证后即可注销。

百度将在不超过 15 个工作日内完成核查和处理，用户注销帐号后，百度将根据法律法规要求删除或者匿名化处理用户的个人信息。

用户不喜欢百度推荐的个性化新闻、广告等内容，如何调整关闭？

用户可点击推荐内容右下角“×”按钮，选择“不感兴趣”，之后百度将会减少相关推荐。
针对所有类型的广告，用户均可通过“设置”—“广告屏蔽”开关，智能 / 手动屏蔽网站广告；
也可通过“设置”—“隐私设置”—“程序化广告设置”屏蔽信息流中第三方程序化广告。

如何删除搜索历史？

在百度 App 首页点击搜索框进入搜索页，搜索框下方的搜索历史记录—旁边的“垃圾箱”按钮，删除历史记录即可。搜索历史是本地数据，一旦清理无法恢复。

用户作品被侵权抄袭，如何维权？

如果用户原创作品被抄袭，用户准备好相关材料后可在 http://copyright.baidu.com“版权投诉”模块进行投诉，收到用户的投诉后百度会尽快处理。

用户访问页面过程中为什么会有安全警告提示？如何消除？

百度特设置安全警告以提醒用户访问的网站可能存在安全问题，该警告无法完全消除或关闭。如果用户浏览的网页频繁弹出安全警告，用户可将浏览网页的搜索词、截图和页面链接，提交至“我的”—“帮助与反馈”—“产品建议”页面中，百度会尽快处理。

如何在“百度知道”设置前台匿名问答或隐藏问答？

用户在百度知道 PC 端及 App 端提交问题或答案时，选择勾选编辑器下方“匿名”即可设置前台匿名问答。问答内容将会以匿名或者热心网友的形式出现，不会在前台显示用户的 ID 名称。另外，用户可以在百度知道 App 端点击右上角“设置”—“隐私设置”，针对“我的提问可见 / 我的回答可见”进行设置，隐藏问答。

本报告采用环保纸张印刷





地址：北京市海淀区上地十街 10 号百度大厦
邮编：100085
邮箱：esg@baidu.com